NSP selection process

Current status

TCCG

4 December 2018

ECB, Frankfurt am Main

Agenda

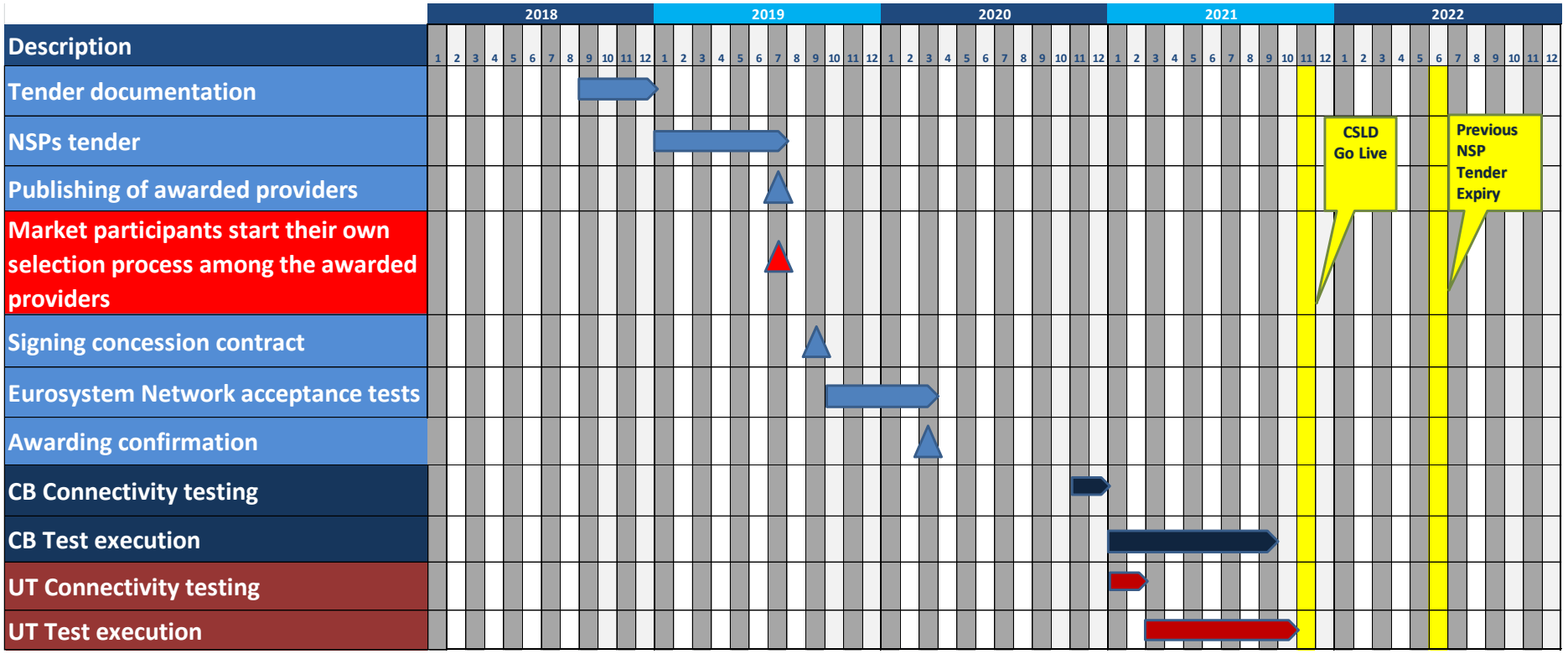
1. Planning
   - Updates
   - NSP tender selection process
   - NSP concession contract relevant milestones
2. NSP tender main new requirements
   - Low volume access and contingency
   - Remote HSM
   - Resending SnF
   - Cold Restart

Planning
Updates

The most relevant updates on the NSP selection process plan are reported below

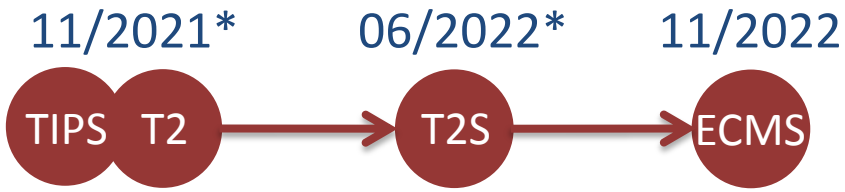
- **Publishing of awarded providers** is now planned in **July 2019** (previously December 2019) *The Market participants can start their own selection process*
- Concession contract will be **signed**, after administrative checks, in **September 2019**
- **Eurosystem Network acceptance tests** process will be completed in **March 2020** (previously June 2020)

Planning
NSP tender selection process



Planning
NSP concession contract relevant milestones

- CSLD go live in Nov 2021
- ECMS go live in Nov 2022
- T2S current License Agreement will expire in June 2022
- TIPS will use NSP concession contract starting from Nov 2021



* The timing as of when the TIPS and T2S will use the NSP concession contract remains to be decided by the MIB.

NSP tender main new requirements
Low volume access and contingency

The new tender shall require NSP to provide, in U2A mode only, a cost-effective access for low payment volume partecipants, with the same service level in place for the fully fledged U2A solution.

The awarded NSPs shall be able to provide both access modes to the Actor (NSP product catalogue will include the U2A low volume access mode).

The low volume access, provided by an alternate NSP, could be used as a contingency in case of primary NSP network failure. This means the «standard» Actor could have two contracts in place:

- a main contract with NSP-1, providing U2A only (small institutions) or both A2A/U2A
- an low volume access contract (U2A only) with NSP-2 in case of contingency

NSP tender main new requirements
Remote HSM

Strong authentication has been implemented in T2S by a two factor authentication:

- something the user knows (PIN)
- something the user owns (smart card or USB token)

This solution implies the usage of a USB port either for the USB Token or for the Smart card reader and specific drivers will have to be installed on the client.

In December 2013 the German National User Group raised CR T2S-0444-BFD (User authentication without USB-token/SmartCard for GUI-access) because of recent constraints on using USB tokens in their organisations

The possibility to adopt remote HSM, as an alternative to USB token/SmartCard, will be encompassed among the technical requirements.

NSP tender main new requirements
Resending SnF

NSP provider will be requested to supply a resending functionality for Store-and-forward traffic (messages and files).

During a predefined period of time, it will be possible to request the NSP to resend Store-and-forward traffic for relevant technical address/es.

NSP tender main new requirements
Cold Restart

In the framework of the current connectivity set up for T2, in case of unavailability of both the OPCs in the European zone, SWIFT guarantees the restart of the service on a third site, with loss of data (so called cold restart).

The current T2S tender does not foresee such requirement for the NSP gateways.

It is proposed to insert such features in the new tender - without limitations on the location of the third site (like today in T2) - for the NSP gateways.

Thank you for your attention